Lena Leffer/Hendrik Mayer

EU-Datenschutz nach „Safe Harbor“

Mit seinem Urteil vom 6. Oktober 2015 hat der EuGH die sog. „Safe Harbor“-Entscheidung der Kommission für ungültig erklärt, die für einen Zeitraum von 15 Jahren von immenser Bedeutung für die Übermittlung personenbezogener Daten aus der EU in die USA war. Dieser Beitrag widmet sich den Hintergründen, dem Nachfolgemodell „EU-US Privacy Shield“ und den hierzu möglichen Alternativen.

Einleitung

In Zeiten zunehmender Globalisierung und wachsender Bedeutung informationstechnischer Dienste hat sich der Datenschutz zu einem grenzüberschreitenden Problem entwickelt. Insbesondere die Übermittlung der auch wirtschaftlich bedeutsamen personenbezogenen Daten aus der EU in die USA kann als *die* datenschutzrechtliche Herausforderung der Gegenwart bezeichnet werden.
Das Recht auf Achtung des Privat- und Familienlebens gem. Art. 7 GR-Charta und das Recht auf Schutz personenbezogener Daten gem. Art. 8 GR-Charta bilden hierbei den europarechtlichen Ausgangspunkt für den Datenschutz in der EU.

Die Richtlinie 95/46/EG

Die Richtlinie 95/46/EG vom 24. Oktober 1995 (Datenschutzrichtlinie, DSRL) stellt dabei den ersten europäischen Rechtsakt zur Harmonisierung auf dem Gebiet des Datenschutzes dar.[1] Die Art. 25 f. DSRL regeln die Übermittlung personenbezogener Daten in Drittländer, d. h. Nicht-EU-Mitgliedstaaten. Die Datenübermittlung ist nach Art. 25 Abs. 1 DSRL nur zulässig, sofern das Drittland ein „*angemessenes Schutzniveau*“ gem. Art. 25 Abs. 2 DSRL gewährleistet. Für Deutschland wurde diese Voraussetzung in § 4b Abs. 2 S. 2 BDSG umgesetzt. Ob ein solches Niveau besteht, kann die Kommission nach Art. 25 Abs. 6 DSRL im Einzelfall per Beschluss feststellen.

Die „Safe Harbor“-Entscheidung der Kommission

Die sog. „Safe Harbor“-Entscheidung stellt den Kommissionsbeschluss 2000/520/EG vom 26. Juli 2000[2] dar, der mehreren seitens des US-Handelsministeriums vorgelegten Dokumenten zustimmte und bei Einhaltung der dort niedergelegten Anforderungen ein angemessenes Datenschutzniveau für in die USA übermittelte Daten i. S. d. Art. 25 Abs. 6 DSRL attestierte (Art. 1 Abs. 1 der Entscheidung).
Inhaltlich wurde amerikanischen Unternehmen die Möglichkeit eröffnet, sich selbst durch Eintragung in ein vom US-Handelsministerium geführtes Register als „sichere Häfen“ zu zertifizieren. Die Aufnahme in das Register setzte insbesondere eine Selbstverpflichtung der Unternehmen zur Einhaltung von sieben „Grundsätzen des ‚sicheren Hafens‘ zum Datenschutz“ („principles“) und von fünfzehn diese konkretisierenden „Häufig gestellten Fragen“ („FAQ“) voraus (Art. 1 Abs. 2 lit. a der Entscheidung).

Das „Schrems“-Urteil des EuGH

Der zuvor genannte Kommissionsbeschluss wurde durch das sog. „Schrems“-Urteil des EuGH vom 6. Oktober 2015 für ungültig erklärt.[3] Hintergrund war eine Klage des österreichischen Datenschutzaktivisten *Maximilian Schrems* gegen den irischen Data Protection Commissioner, da letzterer die Übermittlung personenbezogener Daten von Facebook Ireland Ltd. an Facebook Inc. (USA) nicht untersagte. Der irische High Court legte dem EuGH die Sache zur Vorabentscheidung vor, woraufhin sich letzterer auch mit der Gültigkeit der „Safe Harbor“-Entscheidung auseinandersetzte (Rn. 67 ff.).
Zunächst stellte der EuGH fest, dass es für ein angemessenes Schutzniveau des Drittlandes nicht eines *identischen*, jedoch eines den hohen Datenschutzstandards der EU *gleichwertigen* Schutzes der übermittelten Daten bedarf (Rn. 72 f.).
Auch ein Modell der Selbstzertifizierung könne dies grds. gewährleisten, jedoch mangele es im vorliegenden Fall an den zur Einhaltung der Grundsätze nötigen, wirksamen Überwachungs- und Kontrollmechanismen der US-Behörden (Rn. 82).[4]
Der EuGH kritisierte außerdem die Möglichkeit, die Geltung der Safe Harbor-Grundsätze zugunsten „der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen (…)“ einschränken zu können (Rn. 84 ff.). Dieser umfassende Ausnahmetatbestand gewähre den amerikanischen Behörden ein *generelles*, faktisch unbeschränktes Zugriffsrecht auf die übermittelten Daten und sei deshalb zu unbestimmt und unverhältnismäßig. Ebendiese Problematik leuchtet besonders vor dem Hintergrund der medienwirksamen Enthüllungsskandale um *Edward Snowden* und das PRISM-Programm der NSA ein.
Zudem mangele es auch an einem wirksamen gerichtlichen Rechtsbehelf zugunsten des einzelnen Bürgers i. S. d. Art. 47 Abs. 1 GR-Charta. Dem Bürger bleibe es verwehrt, gerichtlich Zugang zu den übermittelten Daten zu erlangen und deren Berichtigung oder Löschung zu erwirken (Rn. 95).
Letztlich entziehe der Kommissionsbeschluss den Kontrollstellen der EU-Mitgliedstaaten Einwirkungsbefugnisse zur Einhaltung des Angemessenheitserfordernisses, indem er deren Einschreiten von sehr restriktiven Voraussetzungen abhängig mache (Rn. 101 f.). Die Entscheidung sah nämlich grds. eine Einschätzungsprärogative auf US-Seite und eine bloße Notkompetenz der nationalen Kontrollstellen vor.
Der transatlantische Datenverkehr kann somit nicht mehr auf die „Safe Harbor“-Entscheidung gestützt werden. Die Datenübermittlung in die USA muss unterbleiben, sofern nicht der Nachfolger „EU-US Privacy Shield“ oder Alternativinstrumente den angemessenen Schutz der übermittelten Daten gewährleisten.
Nach deutschem Recht drohen – als Umsetzung des Art. 24 DSRL – bei Zuwiderhandeln gem. § 43 Abs. 2 Nr. 1 i. V. m. § 3

Abs. 4 S. 1, § 43 Abs. 3 S. 1 BDSG Bußgelder in Höhe von bis zu 300.000 €.

Der „EU-US Privacy Shield"

Der sog. „EU-US Privacy Shield" („EU-US Datenschutzschild") wurde erstmalig am 2. Februar 2016[5] vorgestellt. Er soll als neuer Angemessenheitsbeschluss der Kommission gem. Art. 25 Abs. 6 DSRL der „Safe Harbor"-Entscheidung nachfolgen. Ein Entwurf hierzu wurde am 29. Februar 2016 veröffentlicht.[6] Dieser beruht auf einer Reihe von Anhängen, die insb. verbindliche Zusicherungen der USA an die EU in Form einer politischen Einigung enthalten.[7] Die hierdurch niedergelegten Rahmenbedingungen sollen die vom EuGH angesprochenen Kritikpunkte ausräumen und damit ein angemessenes Datenschutzniveau schaffen.
Der Datenschutzschild setzt erneut auf ein System der Selbstzertifizierung der US-Unternehmen anhand von sog. „Privacy Shield Principles". Die US-Behörden haben zugesichert, ihre Kontroll- und Durchsetzungsmechanismen gegenüber den US-Unternehmen zu verstärken. Darüber hinaus soll jährlich die Funktionsweise des Datenschutzschildes durch die Kommission und das US-Handelsministerium überprüft werden. Außerdem wird betont, dass die generellen Zugriffsbefugnisse der US-Behörden aus Gründen der nationalen Sicherheit „klar beschränkt" worden seien, insbesondere durch die sog. „Presidential Policy Directive 28" auf sechs Tatbestände.[8] Die wichtigste Änderung betrifft die Einführung wirksamer Rechtsbehelfe zugunsten der EU-Bürger. Zunächst müssen US-Unternehmen Beschwerden von EU-Bürgern innerhalb von 45 Tagen nachgehen. Die Einrichtung einer unabhängigen Ombudsstelle im US-Außenministerium soll sich den Beschwerden von EU-Bürgern gegen behördliche Datenzugriffe widmen. Zusätzlich wurden ein kostenloses Verfahren der alternativen Streitbeilegung und – als ultima ratio – ein Schiedsverfahren zugesichert.

Privacy-Shield: Die EU-Kommission hat gesprochen.

Der Vizepräsident der EU-Kommission, *Andrus Ansip*, hat den „EU-US-Privacy Shield" ausdrücklich für dessen „signifikante Verbesserungen" gelobt.[9]
Seit seiner Vorstellung sieht sich der Datenschutzschild jedoch auch erheblicher Kritik ausgesetzt. Besonders auffallend ist, dass der Datenschutzschild aus einer Sammlung von Dokumenten besteht, die allenfalls eine politische Verbindlichkeit der USA begründen.[10] Die EU ist letztlich von den Zusicherungen der US-Behörden und dem Vertrauen auf deren tatsächliche Durchführung abhängig. Häufig kritisiert wurde auch die fehlende Transparenz der neuen Regelungen.[11] Weitere Kritikpunkte hat die Artikel-29-Datenschutzgruppe (vgl. Art. 29 DSRL) in ihrer Stellungnahme vom 13. April 2016 (vgl. Art. 30 Abs. 1 lit. c DSRL) geäußert. Zum einen seien die Zugriffstatbestände zugunsten der US-Behörden zwar zahlenmäßig beschränkt worden, jedoch inhaltlich immer noch sehr weit und unbestimmt.[12] Weiterhin bestünden erhebliche Zweifel an der Unabhängigkeit der Ombudsstelle und deren effektiven Durchsetzungsmöglichkeiten.[13]
Ein endgültiger Kommissionsbeschluss erging am 12. Juli 2016[14] und wurde am 1. August 2016 im Amtsblatt veröffentlicht.[15] Nach der heftigen Kritik im Vorfeld und einem weiterhin kritischen Statement der Artikel-29-Datenschutzgruppe[16] ist mit einer erneuten Klage vor dem EuGH mit Sicherheit zu rechnen.[17]

Mögliche Alternativen

Neben dem Datenschutzschild sind mehrere Alternativen denkbar, die eine Datenübermittlung in die USA legitimieren können. Diese erlangen insbesondere Relevanz, sollte auch der Datenschutzschild für ungültig erklärt werden.
Art. 26 Abs. 1 DSRL (vgl. § 4c Abs. 1 S. 1 BDSG) sieht Ausnahmen vom Erfordernis eines angemessenen Datenschutzniveaus des Drittlandes vor. Eine solche stellt insb. eine vom Betroffenen ohne jeden Zweifel erklärte *Einwilligung* in die Datenübermittlung dar. Diese muss gem. Art. 2 lit. h DSRL ohne Zwang und in Kenntnis der Sachlage erfolgen und auf eine konkrete Übermittlung bezogen sein.
Gem. Art. 26 Abs. 2 DSRL (vgl. § 4c Abs. 2 BGSG) sind zudem mitgliedstaatliche Genehmigungen von Datenübermittlungen in Drittländer möglich, sofern die übermittelnde Stelle *„ausreichende Garantien"* für den Datenschutz bietet.

INFORMATIONEN ZU DEN AUTOREN

Lena Leffer, Studentische Mitarbeiterin an der juris-Stiftungsprofessur für Rechtsinformatik, *Prof. Dr. Christoph Sorge*, und am Center for IT-Security, Privacy and Accountability (CISPA), Universität des Saarlandes, lena.leffer@uni-saarland.de

Hendrik Mayer, Studentischer Mitarbeiter am Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Arbeitsrecht sowie Privatversicherungsrecht, *Prof. Dr. Roland Michael Beckmann*, Universität des Saarlandes, hendrik.mayer@uni-saarland.de

Solche Garantien können insbesondere in Vertragsklauseln von Datenexporteur und -importeur bestehen, die materielle Datenschutzpositionen und deren Durchsetzung betreffen.[18]
Durch die Verwendung von sog. „*Standardvertragsklauseln*" kann die Datenübermittlung ermöglicht werden, ohne dass die nationalen Aufsichtsbehörden die Genehmigung verweigern dürfen.[19]
Dass die Standardvertragsklauseln ausreichende Datenschutzgarantien beinhalten, wurde gem. Art. 26 Abs. 4 DSRL durch die Kommission festgestellt.[20]
Als weiteren Fall „ausreichender Garantien" i. S. d. Art. 26 Abs. 2 DSRL sieht § 4 Abs. 2 S. 1 BDSG außerdem explizit sog. „verbindliche Unternehmensregelungen" („*Binding Corporate Rules*", BCR) vor.[21] Diese betreffen die konzerninterne Einhaltung von Datenschutzstandards.[22] Die Artikel-29-Datenschutzgruppe hat u. a. eine Checkliste zu notwendigen Inhalten veröffentlicht.[23]

Ausblick: Datenschutzgrundverordnung

Die am 24. Mai 2016 in Kraft getretene und ab 25. Mai 2018 geltende Datenschutzgrundverordnung (DSGVO)[24] regelt die Datenübermittlung an Drittländer in den Art. 44 bis 50. Im Wesentlichen hält sie am Erfordernis eines Angemessenheitsbeschlusses, geeigneter Garantien oder einer Einwilligung fest. Die Sicherstellung der Zulässigkeit der Datenübermittlung erlangt mit der DSGVO außerdem noch größere Brisanz, da gem. Art. 83 Abs. 5 lit. c DSGVO Geldbußen von bis zu 20.000.000 € oder 4 % des weltweiten Vorjahresumsatzes möglich werden.


Lena Leffer, stud. iur., Universität des Saarlandes, Saarbrücken
lena.leffer@uni-saarland.de


Hendrik Mayer, stud. iur., Universität des Saarlandes, Saarbrücken
hendrik.mayer@uni-saarland.de

1 Abl. (EG) v. 23.11.1995, Nr. L 281/31; hierzu *Kühling/Seidel/Sivridis*, Datenschutzrecht, 3. Auflage 2015, Rn. 53 ff.
2 Abl. (EG) v. 25.8.2000, Nr. L 215/7.
3 EuGH, Urteil v. 6.10.2015 – C-362/14 – „Schrems", abrufbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=162125 (zuletzt abgerufen am 4.8.2016).
4 *Borges*, Datentransfer in die USA nach Safe Harbor, NJW 2015, 3617, 3618.
5 Pressemitteilung der Kommission v. 2.2.2016, abrufbar unter http://europa.eu/rapid/press-release_IP-16-216_de.htm (zuletzt abgerufen am 4.8.2016).
6 Pressemitteilung der Kommission v. 29.2.2016, abrufbar unter http://europa.eu/rapid/press-release_IP-16-433_de.htm (zuletzt abgerufen am 4.8.2016).
7 Factsheet der Kommission v. 29.2.2016, abrufbar unter http://europa.eu/rapid/press-release_MEMO-16-434_de.htm (zuletzt abgerufen am 4.8.2016).
8 Vgl. Anhang 6 zur Pressemitteilung v. 29.2.2016 (Fn. 6); *Grau/Granetzny*, EU-US-Privacy Shield – Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?, NZA 2016, 405, 406.
9 Rede v. 2.2.2016, abrufbar unter http://europa.eu/rapid/press-release_SPEECH-16-218_en.htm (zuletzt abgerufen am 4.8.2016).
10 *Spies*, EU/US-Datenübermittlungen: Neuer Datenschutzschild – wie sieht er aus und wie geht es weiter?, ZD-Aktuell 2016, 04992.
11 *Kuntz*, EU-Datenschutzbeauftragter kritisiert Privacy Shield, MMR-Aktuell 2016, 378673; *Horstmann*, 1. Hannoverscher Datenschutztag: Datenschutz in der Wirtschaft zwischen Safe Harbor und dem EU-US-Privacy-Shield, ZD-Aktuell 2016, 04193.
12 Working Paper 238, S. 37 ff., abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (zuletzt abgerufen am 4.8.2016).
13 Working Paper 238 (Fn. 12), S. 45 ff.
14 Pressemitteilung der Kommission v. 12.7.2016, abrufbar unter http://europa.eu/rapid/press-release_IP-16-2461_de.htm (zuletzt abgerufen am 4.8.2016).
15 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12.7.2016, Abl. (EU) v. 1.8.2016, Nr. L 207/1.
16 Statement v. 26.7.2016, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf (zuletzt abgerufen am 4.8.2016).
17 Vgl. auch *Spies*, EU-Kommission billigt den EU-US-Privacy-Shield, ZD-Aktuell 2016, 05235; http://www.heise.de/newsticker/meldung/Privacy-Shield-Lob-von-Unternehmen-Kritik-von-Buergerrechtlern-3263523.html (zuletzt abgerufen am 4.8.2016).
18 Umfang im Einzelnen str., vgl. *Dammann/Simitis*, EG-Datenschutzrichtlinie Kommentar, Art. 26 Rn. 14 ff.; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie Kurzkommentar, Art. 26 Rn. 22 f.
19 *Simitis*, in: ders., BDSG, 8. Auflage 2014, § 4c Rn. 37.
20 Kommissionsentscheidungen 2001/497/EG, 2004/915/EG, 2010/87/EU, mit weiteren Dokumenten abrufbar unter http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (zuletzt abgerufen am 4.8.2016).
21 *Simitis* (Fn. 19), § 4c Rn. 59.
22 *Grau/Granetzny* (Fn. 8), NZA 2016, 405, 407.
23 Working Paper 153, abrufbar unter http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/tools/index_en.htm (zuletzt abgerufen am 4.8.2016).
24 Abl. (EU) v. 4.5.2016, Nr. L 119/1.